Responding to Privacy Breaches

Joanne McNabb, Chief
California Office of Privacy Protection

Protecting Privacy Online
A California Identity Theft Summit
April 11, 2007

Overview

- California Office of Privacy Protection
- Breaches, Breaches, Breaches
- Lessons Learned
- Recommended Practices

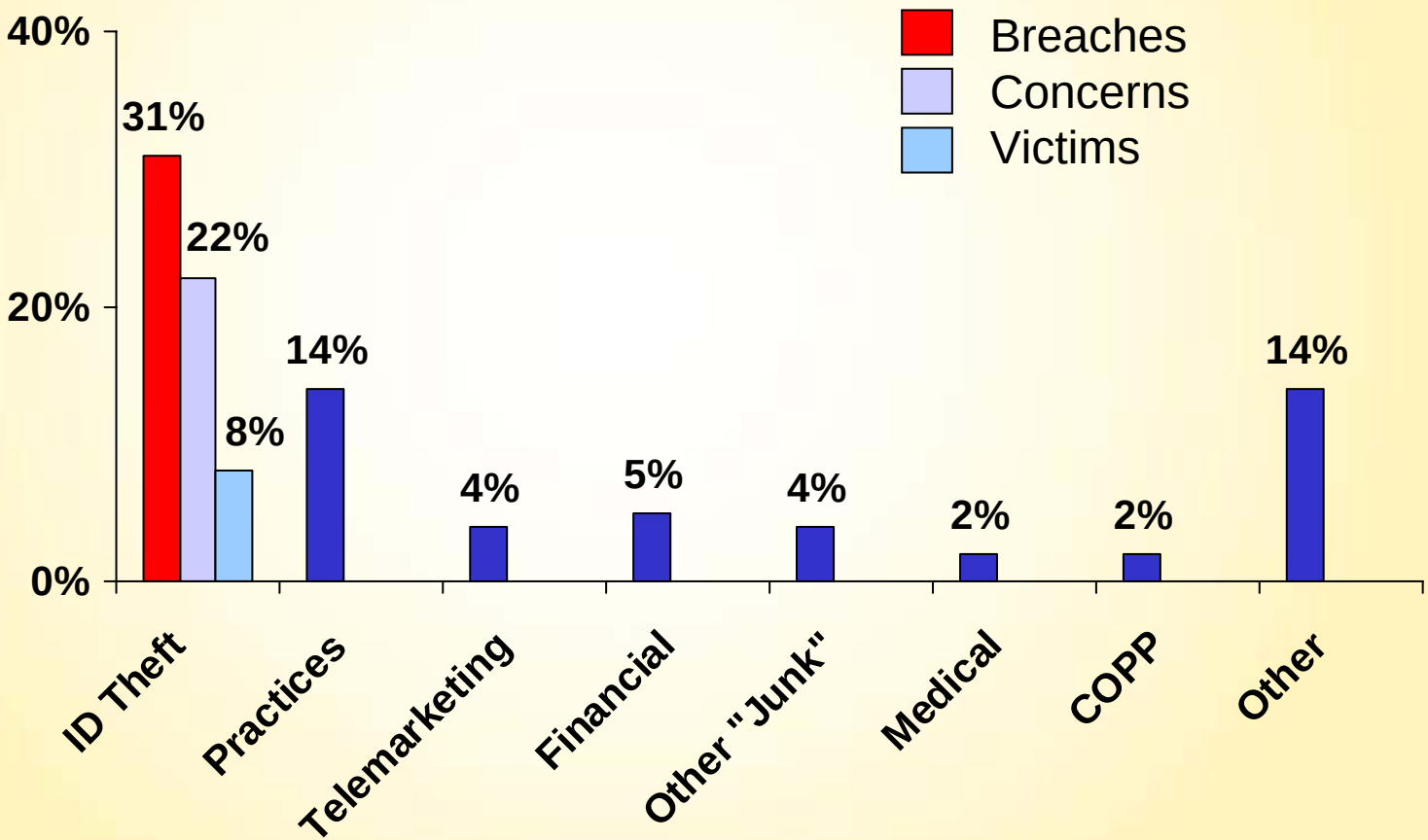
CA Office of Privacy Protection

- Created by law passed in 2000.
  - First in the nation – Now WI too.
- Mission: Protecting the privacy of individuals' personal information … by identifying consumer problems in the privacy area and facilitating the development of fair information practices.

COPP Functions

- Consumer assistance
- Education and information
- Law enforcement coordination and training
- Best practice recommendations

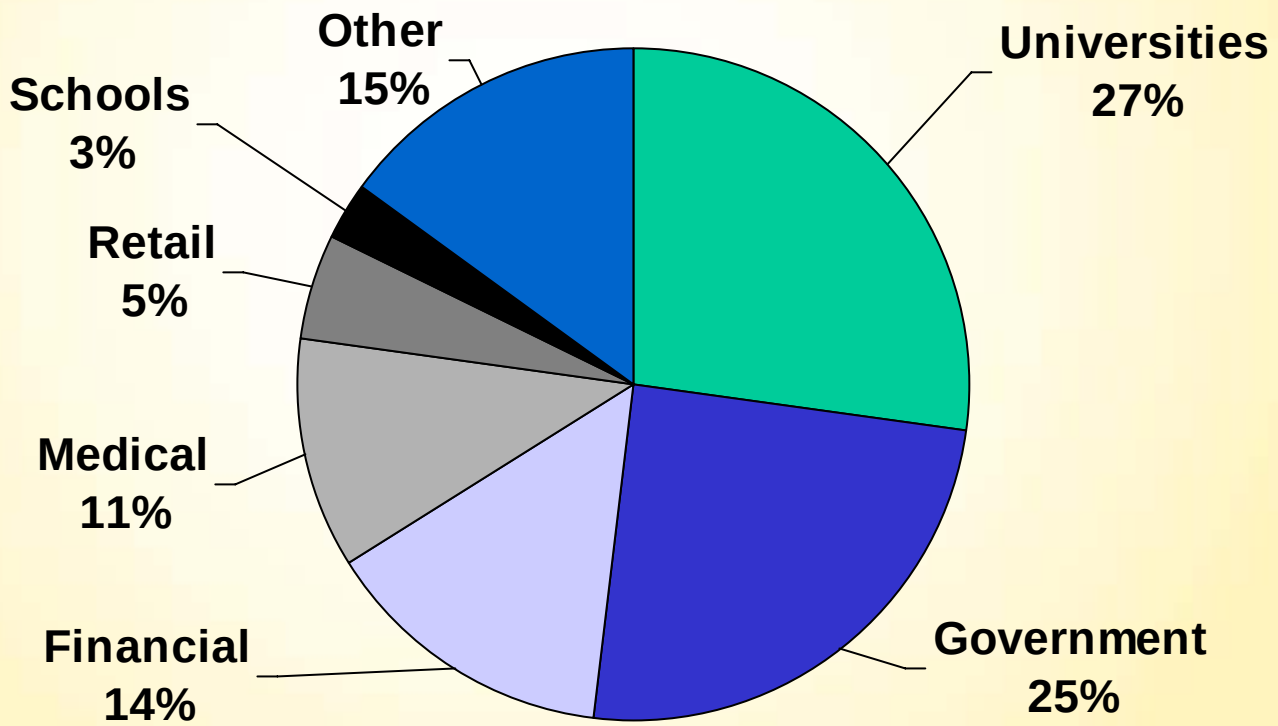
Why People Contact COPP



Security Breaches

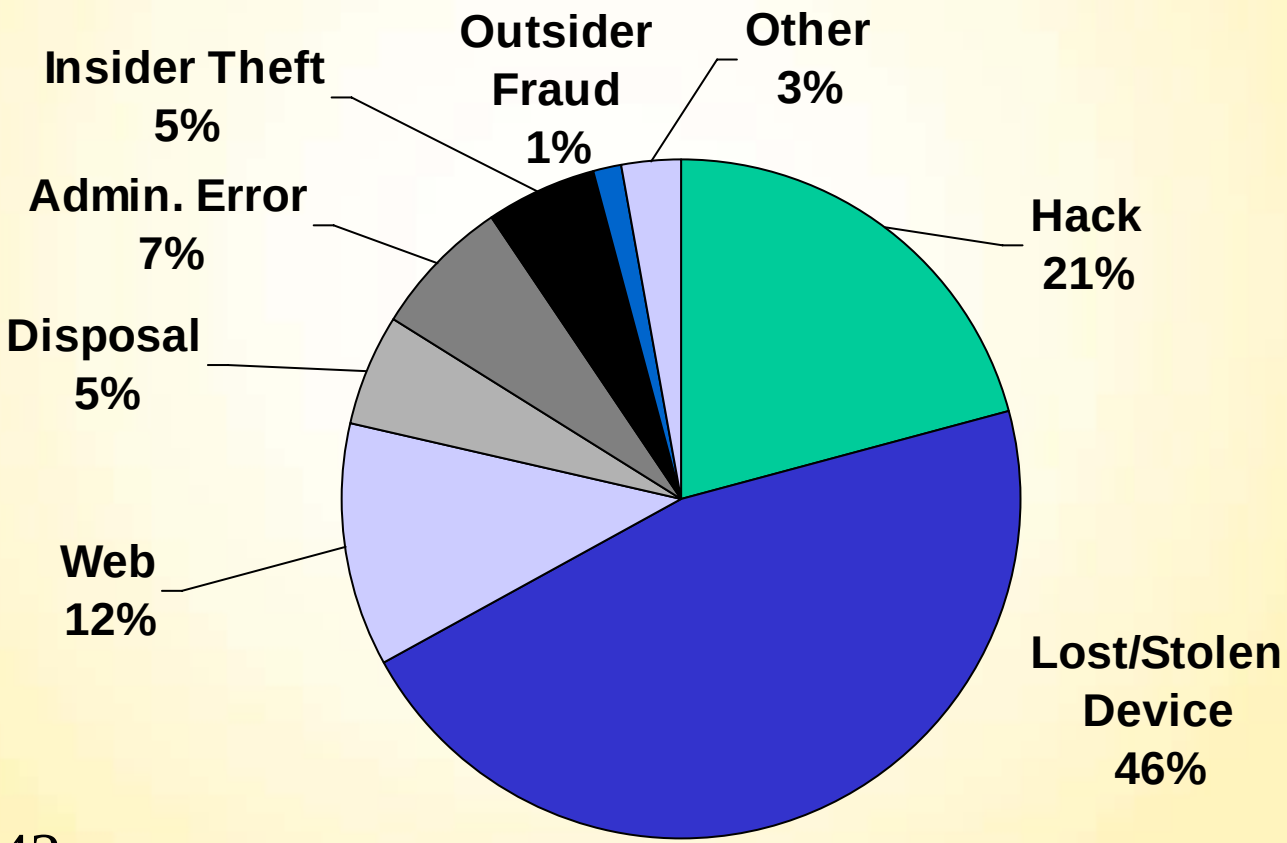
- COPP learns of breaches from consumers who receive notices, companies, state agencies, other organizations, also news media
- Offer assistance (Recommended Practices, Sample Notices, Call Center FAQs), share lessons learned
- Reviewed sample of 542 breach notifications since 2003

Type of Organization



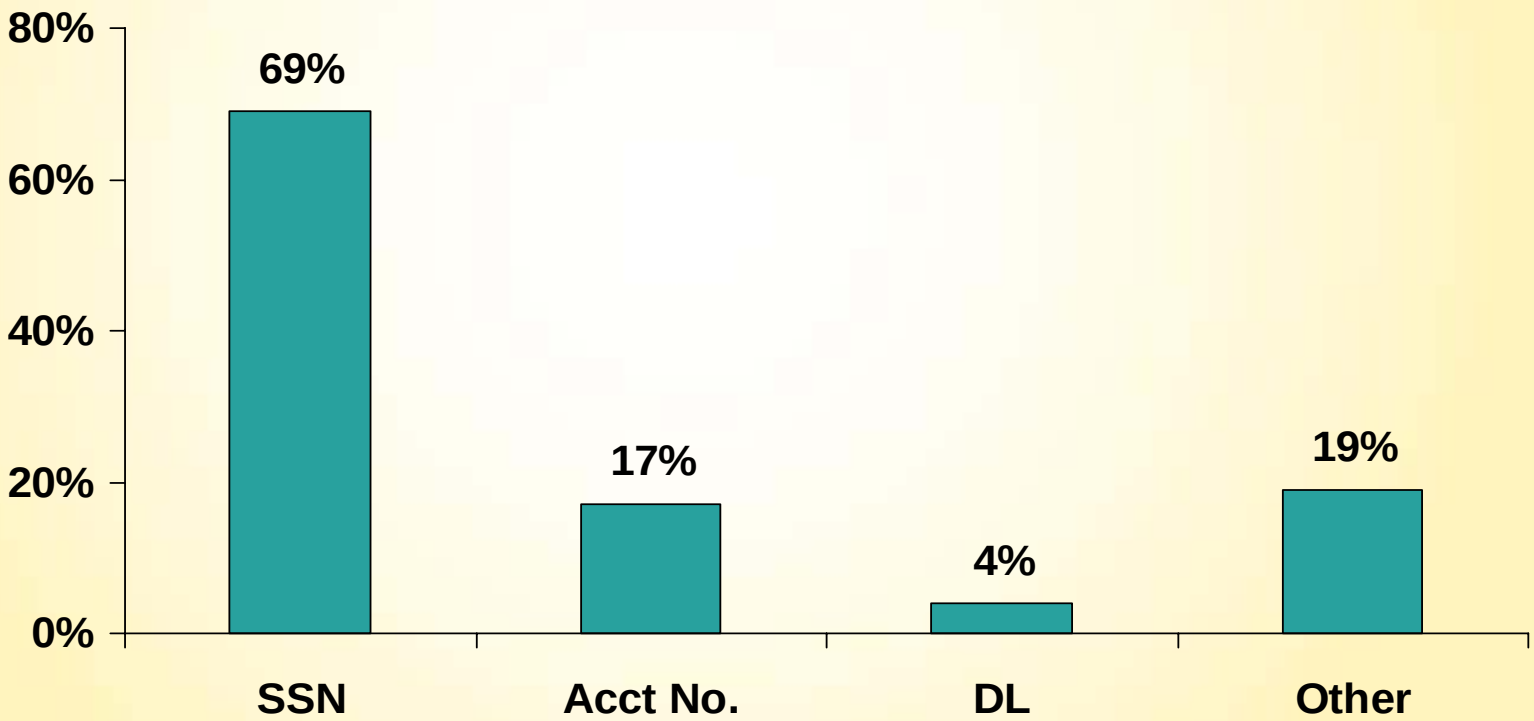
n=542

Type of Breach



n=542

Type of Data Involved



Lessons in Prevention

- Review your data collection policies.
  - Example: Blood banks
  - Do you really need this data element (especially SSNs)?

Lessons in Prevention

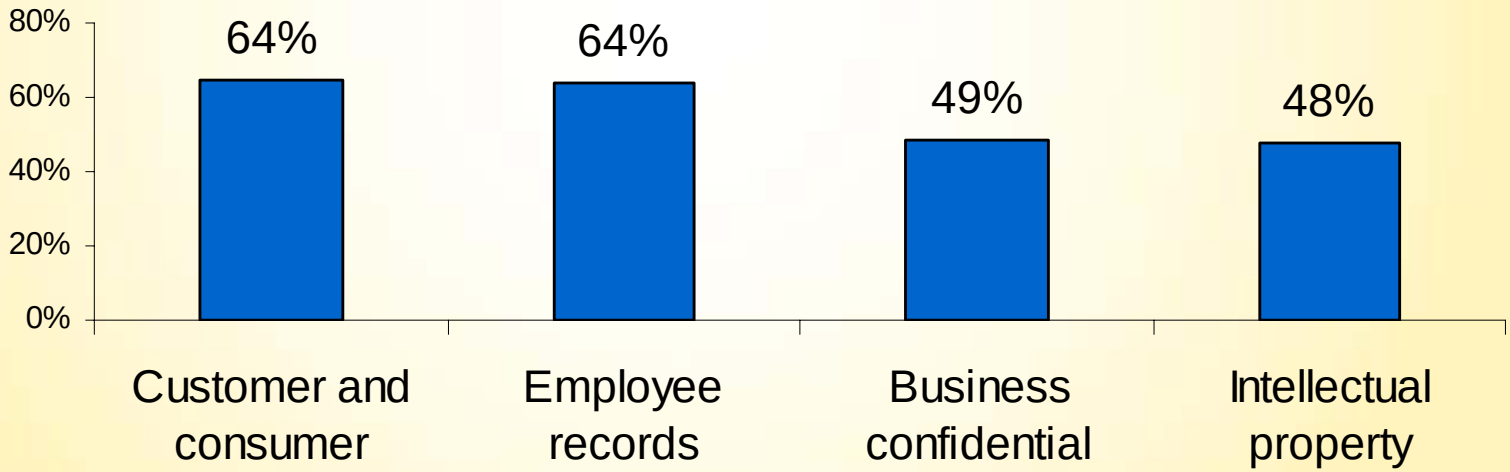
- Review your data retention policies.
  - Example: Universities
  - How long will you need this data (especially SSNs)?

Lessons in Prevention

- Inventory Your Personal & Confidential Data
  - Do you know where your PII is?
    - Laptops
    - PCs
    - Flash drives
    - CDs
    - Tapes
    - Paper records too – In unlocked files? Is mail secure?
  - Is confidential data encrypted?

Where Is Your Confidential Data?

When was the last time your organization conducted an inventory of the following kinds of data? Percentage of respondents saying never.



Source: Ponemon Institute, 2006

Lessons in Prevention

- Data is mobile: Protect desktops, laptops, other portables.
  - Encryption – FIPS 197 (NIST Standard)

Lessons in Prevention

- It’s (almost) always the people!
  - Train everyone – janitors to CEO.
  - Train, train, and train again.
    - Basic practices – Dos and Don’ts.
    - Link to preventing identity theft and retaining customer trust.
    - Role-based training as appropriate.

Lessons in Preparation

- Make sure employees *and contractors* know how to report an info security incident.
  - Single point of contact (CPO, CISO).
  - Over-report – any incident potentially involving data.
- Identify appropriate law enforcement contacts in advance.
  - See law enforcement info in COPP's *Recommended Practices* document.

Lessons in Notification

- Timing of notice: ASAP
  - COPP recommends within 10 days of discovery.
- Start drafting notice while investigating incident.
- Use plain language in notice – Public Affairs, not Legal.

Lessons in Notification

- Credit monitoring?
  - Not appropriate for account-number-only breaches.
  - Consider Security Freeze for SSN/DL breaches (25 states): Stronger protection and less expensive.
- Prepare your Call Center.
  - See Call Center FAQs on COPP's State Government Web page.

Recommending Privacy Practices

- COPP's Recommended Practices
  - Mandate to recommend "privacy policies and practices that promote and protect the interests of California consumers"
  - "Best practice" recommendations
  - Not regulations or legal interpretations
  - Developed with advisory groups of stakeholders

COPP's Recommended Practices

- Related to California privacy laws
  - Security Breach Notice
    - Civil Code § 1798.82
  - Social Security Number Confidentiality
    - Civil Code §§ 1798.85-1798.86
  - Information-Sharing Disclosures and Privacy Policy Statements (
    - Civil Code § 1798.83 ("Shine the Light") and Business and Professions Code §§ 22575-22579 (Online Privacy Protection Act)

"Personal information is like toxic waste – Managing it requires a high level of skill and training."

Phil Agre, *Technology and Privacy in a New Landscape*

Contact Information

Joanne McNabb, Chief
California Office of Privacy Protection
www.privacy.ca.gov
866-785-9663